Null ideals of matrices over residue class rings of principal ideal domains

Roswitha Rissner*

January 6, 2016

Given a square matrix A with entries in a commutative ring S, the ideal of $S[X]$ consisting of polynomials f with $f(A) = 0$ is called the null ideal of A. Very little is known about null ideals of matrices over general commutative rings. First, we determine a certain generating set of the null ideal of a matrix in case $S = {}^{D}/_{dD}$ is the residue class ring of a principal ideal domain D modulo $d \in D$. After that we discuss two applications. We compute a decomposition of the S-module $S[A]$ into cyclic S-modules and explain the strong relationship between this decomposition and the determined generating set of the null ideal of A. And finally, we give a rather explicit description of the ring $\mathrm{Int}(A, \mathrm{M}_n(D))$ of all integer-valued polynomials on A.

Keywords. null ideal, matrix, minimal polynomial, integer-valued polynomials

2010 Math. Subj. Class. 11C08, 11C20, 13F20, 15A15, 15B33, 15B36

1 Introduction

Matrices with entries in commutative rings arise in numerous contexts, both in pure and applied mathematics. However, many of the well-known results of classical linear algebra do not hold in this general setting. This is the case even if the underlying ring is a domain (but not a field). For a general introduction to matrix theory over commutative rings we refer to the textbook of Brown [4].

The purpose of this paper is to provide a better understanding of null ideals of square matrices over residue class rings of principal ideal domains.

Definition 1.1. Let S be a commutative ring, $A \in \mathrm{M}_n(S)$ an $n\times n$-square matrix A over S. The *null ideal* $\mathsf{N}^S(A)$ of A (over S) is the set of all polynomials which annihilate A,

[*] Graz University of Technology, Department of Analysis and Computational Number Theory, Steyrergasse 30, 8045 Graz, Austria. rissner@math.tugraz.at. Supported by Austrian Science Fund (FWF): P23245-N18

that is,

$$\mathsf{N}^S(A) = \{\, f \in S[X] \mid f(A) = 0 \,\}.$$

We often write $\mathsf{N}(A)$ instead of $\mathsf{N}^S(A)$ if the underlying ring is clear from the context.

In case S is a field, it is well-known that the null ideal of A is generated by a uniquely determined monic polynomial, the so-called *minimal polynomial* μ_A of A. Further, it is known that if S is a domain, then the null ideal of every square matrix is principal (generated by μ_A) if and only if S is integrally closed, (Brown [5], Frisch [9]). However, little is known about the null ideal of a matrix with entries in a commutative ring. The well-known Cayley-Hamilton Theorem states that every square matrix over a commutative ring satisfies its own characteristic equation (cf. [12, Theorem XIV.3.1]). Therefore there always exists a monic polynomial in $S[X]$ of minimal degree which annihilates the matrix.

Definition 1.2. Let $A \in \mathrm{M}_n(S)$ be a square matrix over a commutative ring S. If $f \in S[X]$ is a monic polynomial with $f(A) = 0$ and there exists no monic polynomial in $S[X]$ of smaller degree with this property, then we call f a *minimal polynomial* of A over S.

Note that, in case S is a field, the definition above is consistent with the classical definition of the (uniquely determined) minimal polynomial of a square matrix. However in general, if S is not a field, a minimal polynomial of a matrix over S is not uniquely determined, although its degree is. It is known that if S is a domain, then the null ideal of A is principal if and only if A has a uniquely determined minimal polynomial over S, which is in turn equivalent to the (uniquely determined) minimal polynomial μ_A of A over the quotient field of S being in $S[X]$.
Brown discusses conditions for the null ideal to be principal over a general commutative ring R (with identity). In [7], he gives sufficient conditions on certain $R[X]$-submodules of the null ideal for the null ideal to be principal. There is also earlier work of Brown investigating the relationship of the null ideals of certain pairs of square matrices over a commutative ring (which he refers to as spanning rank partners), see [5], [6].
A better understanding of null ideals of matrices over residue class rings of domains has applications in the theory of integer-valued polynomials on matrix rings. Let D be a domain with quotient field K, and let $A \in \mathrm{M}_n(D)$. For a polynomial $f \in K[X]$, the image $f(A)$ of A under f is a matrix with entries in K. There are two immediate questions in this context: For which $f \in K[X]$ does $f(A) \in \mathrm{M}_n(D)$ hold? And what are the images of A under these polynomials? We set

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \{\, f \in K[X] \mid f(A) \in \mathrm{M}_n(D) \,\}$$

the ring of integer-valued polynomials on A, and we denote by

$$\text{Int-Im}(A, \mathrm{M}_n(D)) = \{\, f(A) \mid f \in \mathrm{Int}(A, \mathrm{M}_n(D)) \,\}$$

the ring of images of A under integer-valued polynomials of A. $\mathrm{Int}(A, \mathrm{M}_n(D))$ is an overring of the ring of integer-valued polynomials on the D-algebra $\mathrm{M}_n(D)$, that is,

$$\mathrm{Int}(\mathrm{M}_n(D)) = \{\, f \in K[X] \mid f(\mathrm{M}_n(D)) \subseteq \mathrm{M}_n(D) \,\}.$$

The ring $\mathrm{Int}(\mathrm{M}_n(D))$ and other generalizations of integer-valued polynomial rings are subject of recent research, see [8], [10], [11], [13], [14] and [15].
The connection between integer-valued polynomials on a matrix and null ideals of matrices is the following: Let $f \in K[X]$, then there exist $g \in D[X]$ and $d \in D$ such that $f = g/d$. The following assertion holds:

$$\forall\, d \in D \setminus \{0\} \;\; \forall\, g \in D[X] \;:\; \Big(\frac{g}{d} \in \mathrm{Int}(A, \mathrm{M}_n(D)) \iff g(A) \equiv 0 \mod d\,\mathrm{M}_n(D)\Big)$$

which is the case if and only if the residue class of g is in the null ideal of A over the residue class ring ${}^{D}\!/_{dD}$.
In this paper, we investigate the null ideal of a square matrix A over the residue class ring ${}^{D}\!/_{dD}$ of a principal ideal domain D modulo $d \in D$. In Section 2 we provide a description of a specific set of generators of the null ideal of a matrix with entries in ${}^{D}\!/_{dD}$. With this goal in mind, we generalize the notion of the null ideal at the beginning of the section. Instead of looking only at the ideal of polynomials which map A to the zero ideal, we are also interested in those polynomials which map A to the ideal $d\,\mathrm{M}_n(D)$, cf. Definition 2.1. This point of view has the advantage that it allows us to work over domains instead of residue class rings (which, in general, have zero-divisors). Further, it turns out that it suffices to consider the special case when $d = p^\ell$ is a prime power ($\ell \in \mathbb{N}$ and $p \in D$ a prime element). The main result of this section is Theorem 2.19 which describes a specific set of generators of the null ideal of a matrix over ${}^{D}\!/_{p^\ell D}$. However, this description is theoretic; so far, we do not know how to determine them algorithmically in general. It is possible to compute these generators explicitly in case of diagonal matrices. We present this approach at the end of Section 2.
The theoretical results in Section 2 allow us to present two applications. In Section 3 we analyze the ${}^{D}\!/_{p^\ell D}$-module structure of ${}^{D}\!/_{p^\ell D}[A]$ for $A \in \mathrm{M}_n({}^{D}\!/_{p^\ell D})$. As a finitely generated module over a principal ideal ring, ${}^{D}\!/_{p^\ell D}[A]$ decomposes into a direct sum of cyclic submodules with uniquely determined invariant factors, according to [4, Theorem 15.33]. We describe this decomposition explicitly and find a strong relationship to the generating set of $\mathsf{N}^{D/p^\ell D}(A)$ from Section 2. This allows us to find certain invariant properties of this generating set.
In the last section we apply the knowledge about the null ideal gained in Section 2 to integer-valued polynomials. We give an explicit description of the ring $\mathrm{Int}(A, \mathrm{M}_n(D))$ using the generating set of the null ideal of A modulo finitely many prime powers p^ℓ. Once this description is given, the ring $\text{Int-Im}(A, \mathrm{M}_n(D))$ of images of A under integer-valued polynomials is easily determined.

2 Generators of the null ideal

As already mentioned in the introduction, the goal of this section is to compute a generating set of the null ideal of a square matrix over residue class rings of a principal ideal domain D. However, as it is much more convenient to work over domains instead of residue class rings (which, in general, contain zero-divisors) it turns out to be useful to generalize the notion of the null ideal of a matrix. Instead of investigating only ideals of polynomials which map a given matrix to the zero ideal, we are also interested in polynomials which map the matrix to the ideal $J\,\mathrm{M}_n(D)$ where J is an ideal of D. Although the results in this paper are restricted to matrices over principal ideal domains and their residue class rings, the following definitions make sense in much broader generality. Therefore, up to and including Remark 2.6, we allow the underlying ring to be a general commutative ring.

Definition 2.1. Let S be a commutative ring, J an ideal of S and $A \in \mathrm{M}_n(S)$ a square matrix. We call

$$\mathsf{N}_J^S(A) = \{\, f \in S[X] \mid f(A) \in J\,\mathrm{M}_n(S)\,\}$$

the *J-ideal of A* (over S). Further, we say f is a *J-minimal polynomial of A* (over S), if f is a monic polynomial in $\mathsf{N}_J^S(A)$ and $\deg(f) \le \deg(g)$ for all monic polynomials $g \in \mathsf{N}_J^S(A)$. If the underlying ring is clear from the context, we often omit the superscript and write $\mathsf{N}_J(A)$ instead of $\mathsf{N}_J^S(A)$.

Remark 2.2. With this definition, the null ideal $\mathsf{N}^S(A)$ of A is just the $\mathbf{0}$-ideal $\mathsf{N}_{\mathbf{0}}^S(A)$ (that is if $J = \mathbf{0}$ is the trivial ideal). Further, the $\mathbf{0}$-minimal polynomials of a matrix A are exactly the minimal polynomials of A over S, cf. Definition 1.2. We often use the more classical notation $\mathsf{N}^S(A)$ (and say minimal polynomial instead of $\mathbf{0}$-minimal polynomial) as it is less technical.

For the remainder of this paper, let the following notation and conventions hold.

Notation and Conventions 2.3. Let S be a commutative ring, J an ideal of S and $A \in \mathrm{M}_n(S)$. We identify the isomorphic rings $\mathrm{M}_n({}^{S}\!/_{J}) = {}^{\mathrm{M}_n(S)}\!/_{J\,\mathrm{M}_n(S)}$ and ${}^{S}\!/_{J}[X] = {}^{S[X]}\!/_{JS[X]}$ and write $[\,.\,]_J$ to denote residue classes modulo J.

Remark 2.4. The null ideal $\mathsf{N}^{S/J}([A]_J)$ of the residue class $[A]_J \in \mathrm{M}_n({}^{S}\!/_{J})$ of A modulo J is the image of the J-ideal $\mathsf{N}_J^S(A)$ of A under the projection modulo J, that is,

$$\mathsf{N}^{S/J}([A]_J) = \mathsf{N}_{\mathbf{0}}^{S/J}([A]_J) = \{\, [f]_J \in {}^{S}\!/_{J}[X] \mid f \in \mathsf{N}_J^S(A)\,\}.$$

Remark 2.5. Whether a monic polynomial $f \in S[X]$ is a J-minimal polynomial of A depends only on the residue class of A modulo J. If $J \neq S$ is a proper ideal, then a monic polynomial $f \in S[X]$ is a J-minimal polynomial if and only if its residue class $[f]_J \in {}^{S}\!/_{J}[X]$ is a $\mathbf{0}$-minimal polynomial of $[A]_J$ over ${}^{S}\!/_{J}$. (In case $J = S$, one would have to think about the meaning of “monic” polynomial over the null ring to state a similar result. As we do not want to consider the zero polynomial to be monic, we exclude this case.) Further, let I be an ideal of S such that $I \subseteq J$. Then ${}^{S}\!/\!{}_{J} \simeq {}^{(S/I)}\!/\!{}_{(J/I)}$. Therefore, f is a J-minimal polynomial of A over S if and only if $[f]_I \in {}^{S}\!/\!{}_{I}[X]$ is a ${}^{J}\!/\!{}_{I}$-minimal polynomial of $[A]_I$ over ${}^{S}\!/\!{}_{I}$.

Remark 2.6. The S-ideal $\mathsf{N}_S^S(A)$ of every square matrix A over S is just the whole ring $S[X]$ (that is, if $J = (1) = S$ is the unit ideal). It is therefore generated by the constant polynomial 1. Hence the constant 1 is the (uniquely determined) S-minimal polynomial of every square matrix A over S.

As stated at the beginning of this section, for the remainder of this paper we restrict the underlying ring to be a principal ideal domain. Hence, from this point on, the following notation and conventions hold.

Notation and Conventions 2.7. Let D be a principal ideal domain and $\mathbb{P}$ be a complete set of representatives of associate classes of prime elements of D. Note that $J = (d)$ for some $d \in D$. We write $\mathsf{N}_d(A)$ instead of $\mathsf{N}_{(d)}(A)$ (and omit the superscript D). For the residue classes modulo d, we often write $[\,.\,]_d$ instead of $[\,.\,]_{(d)}$.

The first result of this section is the following lemma. It states a simple but crucial relation between the degrees and the leading coefficients of polynomials in the (d)-ideal of a matrix. Observe that if the leading coefficient of a polynomial $g \in D[X]$ (denoted by $\mathsf{lc}(g)$) is coprime to d, then it is a unit modulo d. Hence, there exists an element $c \in D$ such that $[cg]_d$ is a monic polynomial in ${}^{D}\!/\!{}_{dD}[X]$. In particular, this implies the following lemma.

Lemma 2.8. *Let D be a principal ideal domain and $d \in D$ with $d \notin \{0, 1\}$. If $f \in D[X]$ is a (d)-minimal polynomial, then all polynomials $g \in \mathsf{N}_d(A)$ with $\deg(g) < \deg(f)$ have a leading coefficient $\mathsf{lc}(g)$ which is not invertible modulo d, that is, $\gcd(\mathsf{lc}(g), d) \neq 1$.*

Recall that $\mathsf{N}_0(A) = \mathsf{N}(A)$ is the null ideal of A over D. Further, D is integrally closed, since it is a principal ideal domain. As mentioned in the introduction, this implies that the minimal polynomial of every square matrix in $\mathrm{M}_n(D)$ is in $D[X]$ and generates its null ideal. In particular,

$$\mathsf{N}_0(A) = \mathsf{N}(A) = \mu_A D[X]$$

holds, where $\mu_A \in D[X]$ is the minimal polynomial of A over K. This completes the case $d = 0$. For $d \neq 0$, we first observe, that it suffices to compute $\mathsf{N}_d(A)$ for $d = p^\ell$ with $p \in D$ a prime element and $\ell \in \mathbb{N}$.

Lemma 2.9. *Let D be a principal ideal domain, $A \in \mathrm{M}_n(D)$ and $a, b \in D$ be coprime elements. Then*

$$\mathsf{N}_{ab}(A) = a\,\mathsf{N}_b(A) + b\,\mathsf{N}_a(A).$$

Proof. The inclusion "$\supseteq$" is trivial. For "$\subseteq$", let $g \in \mathsf{N}_{ab}(A)$. Since a and b are coprime, there exist $h_1, h_2 \in D[X]$ such that

$$g = ah_1 + bh_2.$$

Then

$$\begin{aligned} ah_1(A) &= g(A) - bh_2(A) \in b\,\mathrm{M}_n(D) \text{ and} \\ bh_2(A) &= g(A) - ah_1(A) \in a\,\mathrm{M}_n(D). \end{aligned}$$

It follows that $h_1 \in \mathsf{N}_b(A)$ and $h_2 \in \mathsf{N}_a(A)$, which completes the proof. □

Notation and Conventions 2.10. For the rest of this section we fix the prime element $p \in D$. If $A \in \mathrm{M}_n(D)$ is fixed, we often write N_{p^ℓ} instead of $\mathsf{N}_{p^\ell}(A)$.

Our goal is to determine polynomials $f_0, \dots, f_m \in D[X]$ such that

$$\mathsf{N}_{p^\ell}(A) = \{\, f \in D[X] \mid f(A) \equiv 0 \bmod p^\ell \,\} = \sum_{i=0}^{m} f_i D[X]$$

for $A \in \mathrm{M}_n(D)$. Since ${}^{D}\!/_{pD}$ is a field, the null ideal of A modulo p is a principal ideal. Hence

$$\mathsf{N}_p(A) = \nu_1 D[X] + pD[X]$$

where ν_1 is a (p)-minimal polynomial of A. The degree of ν_1 is, by definition, independent of the choice of a (p)-minimal polynomial.

Definition 2.11. Let $\nu_1 \in D[X]$ be a (p)-minimal polynomial A. We call $\mathsf{d}_p(A) = \deg(\nu_1)$ *the* p*-degree of* A and write d_p if the matrix is clear from the context.

Note again, that this definition depends only on the residue class of A modulo p, cf. Remark 2.5. Observe that the following inclusions hold

$$\mu_A D[X] = \mathsf{N}(A) = \mathsf{N}_0 \subseteq \cdots \subseteq \mathsf{N}_{p^\ell} \subseteq \mathsf{N}_{p^{\ell-1}} \subseteq \cdots \subseteq \mathsf{N}_p = \nu_1 D[X] + pD[X] \subseteq D[X] = \mathsf{N}_1$$

where ν_1 is a (p)-minimal polynomial of A. The p-degree of A is a lower bound for the degree of all polynomials in $\mathsf{N}_{p^\ell} \setminus p^\ell D[X]$, as the following lemma states.

Lemma 2.12. *Let D be a principal ideal domain, $\ell \geq 1$ and $A \in \mathrm{M}_n(D)$. If $f \in \mathsf{N}_{p^\ell}(A) \setminus p^\ell D[X]$, then* $\deg(f) \geq \mathsf{d}_p(A)$.

Proof. We prove this by contradiction. Let $\ell \geq 1$ be minimal such that there exists a polynomial $f \in \mathsf{N}_{p^\ell} \setminus p^\ell D[X]$ with $\deg(f) < \mathsf{d}_p$. Without restriction, we choose f to be a polynomial of minimal degree with this property, that is, if $g \in \mathsf{N}_{p^\ell}$ with $\deg(g) < \deg(f)$, then $g \in p^\ell D[X]$.
If $\ell = 1$, then p divides $\mathsf{lc}(f)$ according to Lemma 2.8. Hence $f' = \mathsf{lc}(f)X^{\deg(f)} \in pD[X] \subseteq \mathsf{N}_p$, and therefore $f - f' \in \mathsf{N}_p$ is a polynomial with degree strictly smaller than $\deg(f)$. Therefore $f - f' \in pD[X]$ which implies $f \in pD[X]$, a contradiction.
Hence $\ell > 1$, and since $f \in \mathsf{N}_{p^\ell}$ it follows that $f \in \mathsf{N}_{p^{\ell-1}}$. Then, due to the minimality of ℓ, it follows that $f \in p^{\ell-1}D[X]$. Let $h \in D[X]$ such that $f = p^{\ell-1}h$. Then $\deg(h) = \deg(f) < \mathsf{d}_p$ and

$$f(A) = p^{\ell-1}h(A) \equiv 0 \bmod p^\ell$$

which is equivalent to $h \in \mathsf{N}_p$. Then again, by minimality of $\ell > 1$, it follows that $h \in pD[X]$ and therefore $f \in p^\ell D[X]$, contrary to our assumption.

□

The next proposition provides one of the main tools in this section. It states a simple but important result, which allows us to deduce various properties of the generators of N_{p^ℓ}.

Proposition 2.13. *Let D be a principal ideal domain, $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$ be a square matrix over D, and ν_ℓ be a (p^ℓ)-minimal polynomial of A (for $\ell \geq 1$). If $f \in \mathsf{N}_{p^\ell}(A)$, then there exist uniquely determined polynomials $q, g \in D[X]$ such that* $\deg(g) < \deg(\nu_\ell)$ *and*

$$f = q\nu_\ell + pg.$$

In particular,

$$\mathsf{N}_{p^\ell}(A) = \nu_\ell D[X] + p\,\mathsf{N}_{p^{\ell-1}}(A).$$

Proof. Let $f \in \mathsf{N}_{p^\ell}$. Since ν_ℓ is monic for every $\ell \geq 1$, we can use polynomial division: there exist uniquely determined $q, r \in D[X]$ with $\deg(r) < \deg(\nu_\ell)$ such that

$$f = q\nu_\ell + r. \tag{2.1}$$

It is easily seen that $r \in \mathsf{N}_{p^\ell}$, hence it suffices to prove the following claim.

Claim. Let $r \in \mathsf{N}_{p^\ell}$ with $\deg(r) < \deg(\nu_\ell)$. Then $r \in pD[X]$.

If $\ell = 1$, then the assertion follows from Lemma 2.12. Let $\ell > 1$ be minimal such that the claim is false. Further, choose $r \in \mathsf{N}_{p^\ell}$ with $\deg(r) < \deg(\nu_\ell)$ of minimal degree such that $r \notin pD[X]$. Since $r \in \mathsf{N}_{p^\ell}$ it is in $\mathsf{N}_{p^{\ell-1}}$ too. By minimality of ℓ, there exist $q', g' \in D[X]$ such that

$$r = q'\nu_{\ell-1} + pg'$$

with $\deg(g') < \deg(\nu_{\ell-1})$. Since $r \notin pD[X]$, it follows that $q' \notin pD[X]$. Therefore, there exists $q_1, q_2 \in D[X]$ with $q_2 \neq 0$ and no non-zero coefficient of q_2 is divisible by p such that

$$q' = pq_1 + q_2.$$

Hence r can be written in the following form

$$r = q_1 \underbrace{p\nu_{\ell-1}}_{\in \mathsf{N}_{p^\ell}} + q_2\nu_{\ell-1} + pg' \in \mathsf{N}_{p^\ell}.$$

This, however, implies that $f' = q_2\nu_{\ell-1} + pg' \in \mathsf{N}_{p^\ell}$. Observe, that $\deg(g') < \deg(\nu_{\ell-1})$ which implies that $\mathsf{lc}(f') = \mathsf{lc}(q_2)\,\mathsf{lc}(\nu_{\ell-1}) = \mathsf{lc}(q_2)$ is not divisible by p. On the other hand,

$$\deg(f') = \deg(q_2) + \deg(\nu_{\ell-1}) \leq \deg(r) < \deg(\nu_\ell)$$

which implies, by Lemma 2.8, that p divides $\mathsf{lc}(f')$, a contradiction. □

We state a corollary of Proposition 2.13, which is particularly useful: the smaller the degree of a polynomial in N_{p^ℓ}, the higher the power of p that divides it.

Corollary 2.14. *Let D be a principal ideal domain and $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$, $\ell \geq 1$, and ν_j be (p^j)-minimal polynomials of A for $1 \leq j \leq \ell$. If $f \in \mathsf{N}_{p^\ell}(A)$, then*

$$\deg(f) < \deg(\nu_j) \quad \Longrightarrow \quad f \in p^{\ell-(j-1)}D[X].$$

In particular, if $\deg(\nu_\ell) = \deg(\nu_j)$, then

$$\mathsf{N}_{p^\ell}(A) = \nu_\ell D[X] + p^{\ell-(j-1)}\mathsf{N}_{p^{j-1}}(A)$$

holds.

Proof. We use induction on $\ell \geq 1$. Let $f \in \mathsf{N}_{p^\ell}$ with $\deg(f) < \deg(\nu_j) \leq \deg(\nu_\ell)$. Observe, that $f = pg$ for some $g \in \mathsf{N}_{p^{\ell-1}}$, according to Proposition 2.13. Hence if $\ell = j \geq 1$, then the assertion follows. In particular, if $\ell = 1$, then $j = 1$ which proves the basis.
Hence assume $\ell > j > 1$. Then $j \leq \ell - 1$ and we can apply the induction hypothesis to $g \in \mathsf{N}_{p^{\ell-1}}$ and conclude that $g \in p^{\ell-1-(j-1)}D[X]$ which completes the proof. □

At this point, we have enough tools to prove that the polynomials $p^{\ell-i}\nu_i$ generate N_{p^ℓ}. Recall that $\mathsf{N}_1(A) = D[X]$ is generated by the constant polynomial 1 (see Remark 2.6). Therefore the constant polynomial $\nu_0 = 1$ is the (uniquely determined) (p^0)-minimal polynomial of A for all prime elements p.
Again, we use induction on ℓ and $\mathsf{N}_1(A) = \mathsf{N}_{p^0}(A) = D[X] = p^0\nu_0 D[X]$ serves as induction basis. The induction step is an application of Proposition 2.13.

Theorem 2.15. *Let D be a principal ideal domain and $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$ be a square matrix over D, $\ell \geq 0$, and $\nu_j \in D[X]$ be (p^j)-minimal polynomials of A for $0 \leq j \leq \ell$. Then*

$$\mathsf{N}_{p^\ell}(A) = \sum_{j=0}^{\ell} p^{\ell-j}\nu_j D[X].$$

□

Theorem 2.15 states that the null ideal N_{p^ℓ} of A is generated by the $\ell + 1$ polynomials $p^{\ell-i}\nu_i$ for $0 \leq i \leq \ell$. However, in general this is not a minimal generating set. While we are not able to decide which subsets are minimal generating sets, we can still identify some redundant polynomials in $\{\, p^{\ell-i}\nu_i \mid 0 \leq i \leq \ell \,\}$. Note that $\deg(\nu_{i+1}) \geq \deg(\nu_i)$ holds for all $i \geq 0$. It turns out that it suffices to keep one polynomial of each degree in $\{\, \deg(\nu_i) \mid 0 \leq i \leq \ell \,\}$ to generate N_{p^ℓ}. Theorem 2.19 states explicitly, which subsets of $\{\, p^{\ell-i}\nu_i \mid 0 \leq i \leq \ell \,\}$ we might choose. Although the resulting generating set might still

not be minimal, it is strongly connected to a certain decomposition of ${}^{D}/_{p^\ell D}[[A]_d]$ into cyclic ${}^{D}/_{p^\ell D}$-submodules which is the topic of Section 3.
Theorem 2.15 and Corollary 2.14 imply that, if $\deg(\nu_{j+1}) = \deg(\nu_j)$ for some $0 \le j < \ell$, then N_{p^ℓ} is generated by $\{\, p^{\ell-i}\nu_i \mid 0 \le i \le \ell \,\} \setminus \{p^{\ell-j}\nu_j\}$, cf. Theorem 2.19 below. For each $d \in \{\, \deg(\nu_i) \mid 0 \le i \le \ell \,\}$ we want to keep only the largest j such that $\deg(\nu_j) = d$. This motivates the following definition.

Definition 2.16. Let $A \in \mathrm{M}_n(D)$ be a square matrix with (p^i)-minimal polynomials for $1 \le i \le \ell$. Then we call

$$\mathcal{I}_\ell = \{\ell\} \cup \{\, i \mid 0 \le i < \ell, \deg(\nu_i) < \deg(\nu_{i+1}) \,\}$$

the *ℓ-th index set of A (with respect to the prime element p).*

Remark 2.17. The (uniquely determined) degree of a (p^j)-minimal polynomial of A depends only on the residue class of A modulo p^ℓ, not on the choice of a representative.

Remark 2.18. The indices 0 and ℓ are always contained in $\mathcal{I}_\ell$. Further, the ℓ-th index set $\mathcal{I}_\ell$ of A satisfies the following:

1. If $\deg \nu_\ell \neq \deg \nu_{\ell-1}$, then $\mathcal{I}_\ell = \{\ell\} \cup \mathcal{I}_{\ell-1}$.
2. If $\deg \nu_\ell = \deg \nu_{\ell-1}$, then $\mathcal{I}_\ell = \{\ell\} \cup (\mathcal{I}_{\ell-1} \setminus \{\ell-1\})$.

The ℓ-th index set of A contains the information which (p^j)-minimal polynomials we need to generate N_{p^ℓ} as stated by the next theorem.

Theorem 2.19. *Let D be a principal ideal domain, $p \in D$ a prime element and $\ell \ge 0$. Further, let $A \in \mathrm{M}_n(D)$ be a square matrix over D with ℓ-th index set $\mathcal{I}_\ell$ and $\nu_i \in D[X]$ be (p^i)-minimal polynomials for $0 \le i \le \ell$. Then*

$$\mathsf{N}_{p^\ell}(A) = \sum_{i \in \mathcal{I}_\ell} p^{\ell-i}\nu_i D[X].$$

Proof. We prove this by induction on ℓ. If $\ell = 0$, then $\mathcal{I}_0 = \{0\}$ and the assertion follows from Theorem 2.15. Let $\ell \ge 1$. Then $\mathcal{I}_\ell \setminus \{\ell\} \neq \emptyset$; let $k \le \ell - 1$ be the largest index in $\mathcal{I}_\ell \setminus \{\ell\}$. Then $\deg(\nu_\ell) > \deg(\nu_k)$ and $\deg(\nu_\ell) = \deg(\nu_{k+1})$. Corollary 2.14 implies

$$\mathsf{N}_{p^\ell} = \nu_\ell D[X] + p^{\ell-k}\mathsf{N}_{p^k}.$$

However, according to the induction hypothesis,

$$\mathsf{N}_{p^k} = \sum_{i \in \mathcal{I}_k} p^{k-i}\nu_i D[X]$$

holds. In addition, it follows from Remark 2.18 that $\mathcal{I}_\ell = \mathcal{I}_k \cup \{\ell\}$ which completes the proof. □

Remark 2.20. For the general case, let $d = \prod_{i=1}^{m} p_i^{\ell_i}$ be the prime factorization of an element $d \in D$ and $c_i = \prod_{j \neq i} p_j^{\ell_j}$. Let $\nu_{(p,\ell)}$ denote a (p^ℓ)-minimal polynomial and $\mathcal{I}_{(p,\ell)}$ the ℓ-th index set of A with respect to the prime element p. According to Theorem 2.19 and Lemma 2.9, the following holds:

$$\begin{aligned}\mathsf{N}_d(A) &= \sum_{i=1}^{m} \left(\sum_{j \in \mathcal{I}_{(p_i,\ell_i)}} c_i \, (p_i^{\ell_i - j} \nu_{(p_i,j)}) D[X] \right) \\ &= \sum_{i=1}^{m} \left(\sum_{j \in \mathcal{I}_{(p_i,\ell_i)}} \left(\frac{d}{p_i^j} \, \nu_{(p_i,j)} \right) D[X] \right).\end{aligned}$$

The following assertions are technical observations which are useful later-on.

Corollary 2.21. *Let D be a principal ideal domain and $p \in D$ a prime. Further, let $A \in \mathrm{M}_n(D)$ be a square matrix over D with ℓ-th index set $\mathcal{I}_\ell$ (for $\ell \geq 0$) and $\nu_i \in D[X]$ be (p^i)-minimal polynomials of A. If $f \in \mathsf{N}_{p^\ell}(A)$, then*

$$f \in \sum_{i \in \mathcal{I}_\ell^{[f]}} p^{\ell - i} \nu_i \, D[X]$$

where $\mathcal{I}_\ell^{[f]} = \{ \, i \in \mathcal{I}_\ell \mid \deg(\nu_i) \leq \deg(f) \, \}$.

Proof. We prove this by induction on ℓ. Observe that, if $\deg(f) \geq \deg(\nu_\ell)$, then $\mathcal{I}_\ell^{[f]} = \mathcal{I}_\ell$. In this case the assertion holds, according to Theorem 2.19. In particular, this is the case if $\ell = 0$ (which is the induction basis), since $\deg(f) \geq 0 = \deg(\nu_0)$.
Hence assume $\ell \geq 1$ and $\deg(f) < \deg(\nu_\ell)$. Then $\ell \notin \mathcal{I}_\ell^{[f]}$, and, by Corollary 2.14, $f = ph$ with $h \in \mathsf{N}_{p^{\ell-1}}$. According to the induction hypothesis, it follows that

$$h \in \sum_{i \in \mathcal{I}_{\ell-1}^{[h]}} p^{\ell - 1 - i} \nu_i \, D[X].$$

Note that $\deg(f) = \deg(h)$ and therefore $\mathcal{I}_{\ell-1}^{[h]} = \mathcal{I}_{\ell-1}^{[f]}$. We split into two cases, $\deg(\nu_\ell) > \deg(\nu_{\ell-1})$ and $\deg(\nu_\ell) = \deg(\nu_{\ell-1})$. According to Remark 2.18, if $\deg(\nu_\ell) > \deg(\nu_{\ell-1})$, then $\mathcal{I}_{\ell-1} \cup \{\ell\} = \mathcal{I}_\ell$. Since $\ell \notin \mathcal{I}_\ell^{[f]}$ it follows that $\mathcal{I}_{\ell-1}^{[f]} = \mathcal{I}_\ell^{[f]}$.
If $\deg(\nu_\ell) = \deg(\nu_{\ell-1})$, then $\mathcal{I}_\ell = \{\ell\} \cup (\mathcal{I}_{\ell-1} \setminus \{\ell - 1\})$, by Remark 2.18 again. However, $\ell \notin \mathcal{I}_\ell^{[f]}$ and $\ell - 1 \notin \mathcal{I}_{\ell-1}^{[f]}$ since $\deg(f) < \deg(\nu_\ell) = \deg(\nu_{\ell-1})$. Therefore $\mathcal{I}_{\ell-1}^{[f]} = \mathcal{I}_\ell^{[f]}$ in this case too. Hence, in both cases, the following holds:

$$f = ph \in \sum_{i \in \mathcal{I}_\ell^{[f]}} p^{\ell - i} \nu_i \, D[X].$$

□

For $i \geq 1$, let $\nu_i \in D[X]$ be (p^i)-minimal polynomials and $\mu_A \in D[X]$ the minimal polynomial of A. Then, by definition,

$$\mathsf{d}_p = \deg(\nu_1) \leq \cdots \leq \deg(\nu_{\ell-1}) \leq \deg(\nu_\ell) \leq \cdots \leq \deg(\mu_A) = \mathsf{d}_A.$$

In particular, this sequence of degrees stabilizes. The following proposition states that there always exists an m such that every (p^m)-minimal polynomial has degree d_A, that is, the sequence stabilizes always at the value d_A.

Proposition 2.22. *Let D be a principal ideal domain and $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$ with minimal polynomial $\mu_A \in D[X]$ and $\mathsf{d}_A = \deg(\mu_A)$. If ν_i are (p^i)-minimal polynomials of A for $i \geq 0$, then there exists $m \in \mathbb{N}$ such that for all $\ell \geq m$, $\deg(\nu_\ell) = \mathsf{d}_A$ holds.*

Proof. Since $\deg(\nu_i) \leq \deg(\mu_A)$ and $(\deg(\nu_i))_{i\geq 1}$ is a non-decreasing sequence in $\mathbb{N}$, there exists $m \in \mathbb{N}$ such that $\deg(\nu_m) = \deg(\nu_{m+k})$ for all $k \geq 0$. We set $d = \deg(\nu_m)$ and show $d = \mathsf{d}_A$. Note that $d \leq \mathsf{d}_A$, and therefore it suffices to show $d \geq \mathsf{d}_A$.
Since $\nu_{m+k+1} - \nu_{m+k} \in \mathsf{N}_{p^{m+k}}$ is a polynomial with degree less than $\deg(\nu_m)$, it follows from Corollary 2.14 that

$$\nu_{m+k+1} - \nu_{m+k} \in p^{k+1}D[X].$$

For $0 \leq i \leq d$, let $a_i^{(k)}$ be the coefficient of X^i of the polynomial ν_{m+k}. Then $(a_i^{(k)})_{k\geq 0}$ are p-adic Cauchy sequences in D. Therefore $\nu = \lim_{k\to\infty} \nu_{m+k}$ is a polynomial over the p-adic completion $\widehat{D}$ of D with coefficients $a_i = \lim_{k\to\infty} a_i^{(k)}$ and $d = \deg(\nu)$. Since, ν_{m+k} is a monic polynomial for all k, it follows that ν is a monic polynomial too.
Further $\nu(A) = 0$, and hence $\nu \in \mathsf{N}^{\widehat{D}}(A)$. Now, let $\widehat{K}$ be the quotient field of $\widehat{D}$. Then $\widehat{K}$ is a field extension of K. Since the minimal polynomial is invariant under field extensions, it follows that $\mathsf{N}^{\widehat{K}}(A) = \mu_A\widehat{K}[X]$. However, $\widehat{D}$ is integrally closed in $\widehat{K}$, and therefore $\mathsf{N}^{\widehat{D}}(A) = \mu_A\widehat{D}[X]$. Hence $\mu_A \mid \nu$ which implies in particular that $\mathsf{d}_A \leq \deg(\nu) = d$. □

We can conclude, that it suffices to determine a finite number of (p^i)-minimal polynomials in order to describe the ideals $\mathsf{N}_{p^\ell}(A)$ for all $\ell \geq 0$.

Corollary 2.23. *Let D be a principal ideal domain and $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$ and $\mu_A \in D[X]$ the minimal polynomial of A. Then there exists $m \in \mathbb{N}$ such that for all $k \geq 0$ the following holds:*

$$\mathsf{N}_{p^{m+k}}(A) = \mu_A D[X] + p^k \mathsf{N}_{p^m}(A).$$

Proof. For $i \geq 0$, let ν_i be a (p^i)-minimal polynomial of A. Then there exists an $m \in \mathbb{N}$ such that $\deg(\mu_A) = \deg(\nu_{m+1})$, according to Proposition 2.22. Hence, μ_A is a (p^{m+k+1})-minimal polynomial for all $k \geq 0$ and the assertion follows from Corollary 2.14 (with $j = m + 1$). □

2.1 Diagonal matrices

Although we know that (p^ℓ)-minimal polynomials exist, it is in general not clear how to determine them algorithmically. However, in the special case of diagonal matrices it is possible to compute them explicitly. Let $A = \operatorname{diag}(a_1, \ldots, a_n)$ be a diagonal matrix over D, $p \in D$ a prime element, $\ell \in \mathbb{N}$ and $f \in D[X]$ a polynomial. Then $f(A) = \operatorname{diag}(f(a_1), \ldots, f(a_n))$ holds and therefore

$$\forall\, f \in D[X] : \Big(f \in \mathsf{N}_{p^\ell}(A) \quad \iff \quad \forall\, i \in \{1 \ldots, n\} : \; f(a_i) \in p^\ell D \Big) .$$

However, the set of polynomials which maps the elements a_1, …, a_n to multiples of p^ℓ can be determined using Bhargava's p-orderings, cf. [1] and [2]. We explain his approach here in the special case of a principal ideal domain (although it is applicable in the more general case of a Dedekind domain by looking at prime ideals instead of prime elements).

Definition 2.24. Let S be a non-empty subset S of D. A *p-ordering of S* is a sequence $(b_k)_{k\geq 0}$ which is defined iteratively in the following way:

1. Choose $b_0 \in S$ arbitrary.
2. If b_0, …, b_{k-1} are already known, then choose $b_k \in S$ as an element such that $\mathsf{w}_p((b_k - b_0)(b_k - b_1) \cdots (b_k - b_{k-1}))$ is minimal, where w_p denotes the p-adic valuation on D.

In general, there is more than one p-ordering of a set S (except $|S| = 1$) and for each p-ordering $(b_k)_{k\geq 0}$ of S we have the sequence of p powers $p^{\mathsf{w}_p((b_k-b_0)(b_k-b_1)\cdots(b_k-b_{k-1}))}$ (with the usual convention "$p^\infty = 0$"). Bhargava shows that the sequences of p powers of any two p-orderings are the same (cf. [1, Theorem 1]). Hence, these p powers depend only on S and not on the choice of the p-ordering. This motivates the following definition.

Definition 2.25. Let S be a non-empty subset S of D and $(b_k)_{k\geq 0}$ a p-ordering of S. For $k \geq 0$ let

$$v_k(S, p) = p^{\mathsf{w}_p((b_k-b_0)(b_k-b_1)\cdots(b_k-b_{k-1}))} D.$$

Then $(v_k(S, p))_{k\geq 0}$ is called the *associated p-sequence of S*.

Note that $v_0(S, p) = D$. By definition, p-orderings satisfy the following property

$$\forall\, a \in S : \; p^{\mathsf{w}_p((a-b_0)(a-b_1)\cdots(a-b_{k-1}))} \in v_k(S, p). \tag{2.2}$$

Therefore, the associated p-sequence of S forms a descending chain of ideals, that is, $v_{k+1}(S, p) \subseteq v_k(S, p)$ for all $k \geq 0$. In particular, if S is finite, then $v_k(S, p) = \mathbf{0}$ for $k \geq |S| + 1$. Moreover, the property in (2.2) implies that the polynomials of the form $f_k = (X - b_0) \cdots (X - b_{k-1})$ satisfy $f_k(S) \subseteq v_k(S, p)$ for $k \geq 0$. In fact, the polynomials f_k are indeed a suitable choice for our purpose. The following theorem allows us to deduce the desired properties.

Theorem 2.26. *([1, Theorem 11]) Let S be a subset of a principal ideal domain D, and $f \in D[X]$ be a primitive polynomial of degree k. If I_f denotes the smallest ideal of D such that $f(S) \subseteq I_f$, then $v_k(S,p) \subseteq I_f$. Moreover, if $(b_j)_{j\geq 0}$ is a p-ordering of S, then the polynomial*

$$g = (X - b_0)(X - b_1)\cdots(X - b_{k-1})$$

is a polynomials of degree k such that $I_g = v_k(S,p)$.

We can use this theorem to compute (p^ℓ)-minimal polynomials for the diagonal matrix $A = \operatorname{diag}(a_1, \ldots, a_n)$ over principal ideal domains. Let $S = \{a_1, \ldots, a_n\}$ be the set of diagonal elements of A and σ a permutation of $\{1, \ldots, n\}$ such that $(a_{\sigma(i)})_{i=1}^n$ is a p-ordering of S. We set $f_k = (X - a_{\sigma(0)})(X - a_{\sigma(1)})\cdots(X - a_{\sigma(k-1)})$.
For $\ell \in \mathbb{N}$, let k be minimal such that $v_k(S,p) \subseteq p^\ell D$. Then, by Theorem 2.26, $f_k(S) \subseteq p^\ell D$ and we claim that f_k is a (p^ℓ)-minimal polynomial. Assume that $f \in D[X]$ is a monic polynomial with degree less than k and $f(S) \subseteq p^\ell D$. Again by Theorem 2.26, this implies $v_{k-1}(S,p) \subseteq I_f \subseteq p^\ell D$ which contradicts the choice of k.
To compute the (p^ℓ)-minimal polynomial of A we therefore only have to compute a p-ordering of the set of diagonal elements of A. To demonstrate this approach, we conclude this section with an example of a 3×3-matrix over $\mathbb{Z}$.

Example 2.27. Let $A \in \mathrm{M}_3(\mathbb{Z})$ be defined as follows:

$$A = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 16 & 0 \\ 0 & 0 & 32 \end{pmatrix}$$

Then A has three, pairwise different eigenvalues over $\mathbb{Q}$ and hence

$$\mu_A = (X - 4)(X - 16)(X - 32)$$

is the minimal polynomial of A over $\mathbb{Q}$. Since $\mu_A \in \mathbb{Z}[X]$, it is the (in this case uniquely determined) minimal polynomial (or $\mathbf{0}$-minimal polynomial) of A over $\mathbb{Z}$.
Let $p \in \mathbb{Z}$ be a prime element. Recall that we denote the residue classes modulo a prime element p by $[\,.\,]_p$. Then $[A]_p$ has three different eigenvalues in $\mathbb{Z}/p\mathbb{Z}$ for all prime elements in $\mathbb{Z}$ except for the primes 2, 3 and 7. Therefore,

$$\mu_{[A]_p} = (X - [4]_p)(X - [16]_p)(X - [32]_p) \in \mathbb{Z}/p\mathbb{Z}[X]$$

is the minimal polynomial of $[A]_p$ over $\mathbb{Z}/p\mathbb{Z}$ for all $p \in \mathbb{P} \setminus \{2,3,7\}$. This implies $\mathsf{d}_p(A) = \deg(\mu_A)$ for all $p \in \mathbb{P} \setminus \{2,3,7\}$. Therefore μ_A is a (p^ℓ)-minimal polynomial of A and $\{0, \ell\}$ the ℓ-th index set of A with respect to the prime p for all prime elements $p \neq 2,3,7$ and all $\ell \geq 1$. Hence, according to Theorem 2.19,

$$\mathsf{N}_{p^\ell}(A) = \mu_A\mathbb{Z}[X] + p^\ell\mathbb{Z}[X]$$

holds for all $p \in \mathbb{P}\setminus\{2,3,7\}$ and all $\ell \geq 1$. The cases $p = 3$ and $p = 7$ are similar, therefore, we only handle $p = 3$. Observe that $4, 32, 16, 16, \ldots$ is an example of a 3-ordering of the set $\{4, 16, 32\}$ and $D, D, (3), \mathbf{0}, \mathbf{0}, \ldots$ is the associated 3-sequence of this set. Following Bhargava's approach (which we explained above this example), it follows that $f_2 = (X-4)(X-32)$ is a (3)-minimal polynomial and $\mu_A = f_3 = (X-4)(X-32)(X-16)$ is a (3^ℓ)-minimal polynomial $\ell \geq 2$. Moreover, $\{0, 1\}$ is the first and $\{0, 1, \ell\}$ is the ℓ-th index set of A for $\ell \geq 2$ (with respect to 3). Theorem 2.19 implies

$$\mathsf{N}_3(A) = (X-4)(X-32)\,\mathbb{Z}[X] + 3\,\mathbb{Z}[X]$$

and, for all $\ell \geq 2$,

$$\mathsf{N}_{3^\ell}(A) = \mu_A \mathbb{Z}[X] + 3^{\ell-1}(X-4)(X-32)\,\mathbb{Z}[X] + 3^\ell\,\mathbb{Z}[X].$$

It remains to consider the case $p = 2$. The sequence $4, 16, 32, 32, \ldots$ is an example of a 2-ordering of the set $\{4, 16, 32\}$ and $D, (4), (64), \mathbf{0}, \mathbf{0}, \ldots$ is the associated 2-sequence of this set. We use Bhargava's approach again; the results are displayed in Table 2.1.

ℓ	$\mathcal{I}_\ell$	(2^ℓ)-minimal polynomial
1,2	$\{0, \ell\}$	$X - 4$
3,4,5,6	$\{0, 2, \ell\}$	$(X-4)(X-16)$
≥ 7	$\{0, 2, 5, \ell\}$	μ_A

Table 2.1: (2^ℓ)-minimal polynomials of A

Finally, it is worth mentioning that even if the degrees of (p^ℓ)- and $(p^{\ell+1})$-minimal polynomials coincide, a (p^ℓ)-minimal polynomials is in general **not** a $(p^{\ell+1})$-minimal polynomial (while the reverse implication holds). This is easily verified, once one observes that X^2 is both, an (8)- and a (16)-minimal polynomial, but it is not a (32)-minimal polynomial of A.

3 Module structure of ${}^{D}/_{p^\ell D}[A]$

Throughout this section we fix the prime power $p^\ell \in D$ and write R_ℓ for the residue class ring ${}^{D}/_{p^\ell D}$. Let $A \in \mathrm{M}_n(R_\ell)$ be a square matrix with null ideal

$$\mathsf{N} = \mathsf{N}^{R_\ell}(A) = \mathsf{N}_{\mathbf{0}}^{R_\ell}(A) = \{\, f \in R_\ell[X] \mid f(A) = 0 \,\}.$$

Further, let $A' \in \mathrm{M}_n(D)$ be a preimage of A under the projection modulo p^ℓ, that is, $[A']_{p^\ell} = A$ where $[\,.\,]_{p^\ell}$ denotes the residue class modulo p^ℓ (as introduced in Notation and Conventions 2.7). Then, according to Theorem 2.19,

$$\mathsf{N} = \{\, [f]_{p^\ell} \in R_\ell[X] \mid f \in \mathsf{N}_{p^\ell}(A') \,\} = \sum_{i \in \mathcal{I}_\ell \setminus \{0\}} [p]_{p^\ell}^{\ell-i} [\nu_i]_{p^\ell} R_\ell[X]$$

where $\mathcal{I}_\ell$ is the ℓ-th index set of A' and ν_i are (p^i)-minimal polynomials of A' (for $i \in \mathcal{I}_\ell \setminus \{0\}$).

Notation and Conventions 3.1. Let $f' \in D[X]$ be a monic polynomial. Recall that, for $1 \leq j \leq \ell$, f' is a (p^j)-minimal polynomial of A' if and only if $f = [f']_{p^\ell}$ is a $([p^j]_{p^\ell})$-minimal polynomial of A, see Remark 2.5.
For a better readability, we often write p for the residue class $[p]_{p^\ell}$ of p modulo p^ℓ and say that $f \in R_\ell[X]$ is a (p^j)-minimal polynomial of A if it is a $([p^j]_{p^\ell})$-minimal polynomial of A.

Note that the ℓ-th index set of a matrix $A' \in \mathrm{M}_n(D)$ only depends on the residue class of A' modulo p^ℓ, that is, if $A'' \in \mathrm{M}_n(D)$ is a matrix with $[A']_{p^\ell} = [A'']_{p^\ell}$ (and therefore $[A']_{p^j} = [A'']_{p^j}$ for all $1 \leq j \leq \ell$), then A' and A'' have equal ℓ-th index sets, cf. Remark 2.17.

Definition 3.2. Let $A \in \mathrm{M}_n(R_\ell)$ and $A' \in \mathrm{M}_n(D)$ such that $A = [A']_{p^\ell}$. If $\mathcal{I}_\ell$ is the ℓ-th index set of A', then we call $\mathcal{I}_\ell^\star = \mathcal{I}_\ell \setminus \{0, \ell\}$ the *reduced index set of* A. Further, for $i \in \mathcal{I}_\ell \setminus \{\ell\}$, we call $\mathrm{succ}(i) = \min\{i' \in \mathcal{I}_\ell \mid i' > i\}$ the *successor of* i *in* $\mathcal{I}_\ell$.

Remark 3.3. Let $A \in \mathrm{M}_n(R_\ell)$ with reduced index set $\mathcal{I}_\ell^\star$, and let $\nu_i \in R_\ell[X]$ be (p^j)-minimal polynomials of A (for $1 \leq i \leq \ell$). Then $i \in \mathcal{I}_\ell^\star$ if and only if $\deg(\nu_i) < \deg(\nu_{i+1})$, cf. Definition 2.16. Further, note that if $i \in \mathcal{I}_\ell^\star$, then $\deg(\nu_{\mathrm{succ}(i)}) = \deg(\nu_{i+1})$.

In this section we analyze the structure of the R_ℓ-module $R_\ell[A]$. Since the null ideal of A contains a monic polynomial, there exists a power of A which can be written as an R_ℓ-linear combination of smaller powers of A. Therefore the module $R_\ell[A]$ is finitely generated. As a finitely generated module over a principal ideal ring, $R_\ell[A]$ decomposes into cyclic R_ℓ-submodules, according to [4, Theorem 15.33]. We compute such a decomposition exploiting its relation to the generating set of the null ideal N of A which we determined in Theorem 2.19 of the last section. In particular, it turns out that the invariant factors of $R_\ell[A]$ correspond to the elements in the reduced index set $\mathcal{I}_\ell^\star$ of A. Further, their multiplicities relate to the degrees of the (p^j)-minimal polynomials, see Remark 3.6. As the invariant factors are uniquely determined, this corroborates the usefulness of the set of generators of the null ideal of A which we determined in Section 2. To be more specific, Theorem 3.5 below states that, if $\mathcal{I}_\ell^\star$ is the reduced index set of A and $s_j = \deg(\nu_{\mathrm{succ}(j)}) - \deg(\nu_j)$ for $j \in \mathcal{I}_\ell^\star$, then

$$R_\ell[A] \simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{j \in \mathcal{I}_\ell^\star} (R_{\ell-j})^{s_j} \tag{3.1}$$

where $\mathsf{d}_p = \deg(\nu_1)$ is the degree of the minimal polynomial of A modulo p. Roughly speaking, the R_ℓ-free part $R_\ell^{\mathsf{d}_p}$ of the decomposition in (3.1) indicates what happens in terms of classical linear algebra over the field R_1 while the torsion-part of $R_\ell[A]$ relates to the set $\mathcal{I}_\ell^\star$.
In order to understand this connection, let d be the degree of a (p^ℓ)-minimal polynomial ν_ℓ. Then A^d is an R_ℓ-linear combination of I, A, ..., A^{d-1}, and thus $R_\ell[A] = \langle I, A, \ldots, A^{d-1} \rangle_{R_\ell}$. Hence the following sequence of R_ℓ-modules is exact.

$$\begin{array}{ccccccccc} \mathbf{0} & \longrightarrow & \ker(\psi) & \longrightarrow & R_\ell^d & \xrightarrow{\psi} & R_\ell[A] & \longrightarrow & \mathbf{0} \\ & & & & \mathbf{e}_i & \longmapsto & A^{i-1} & & \end{array} \tag{3.2}$$

where $\mathbf{e}_1$, …, $\mathbf{e}_d$ is an arbitrary basis of R_ℓ^d. It follows that

$$R_\ell[A] \simeq {}^{R_\ell^d}\!/_{\ker(\psi)}.$$

Elements of $\ker(\psi)$ correspond to relations between the matrices I, A, …, A^{d-1} and therefore to polynomials in the null ideal N of A of degree less than d. Hence

$$\sum_{i=1}^{d} \lambda_i \mathbf{e}_i \in \ker(\psi) \quad\Longleftrightarrow\quad \sum_{i=1}^{d} \lambda_i X^{i-1} \in \mathsf{N} \tag{3.3}$$

where $\lambda_1, \dots, \lambda_d \in R_\ell$. We exploit this equivalence and use a generating set of the null ideal N of A to compute a generating set of the module $\ker(\psi)$. Nevertheless, we need to be careful, since (as an ideal of $R_\ell[X]$) N is an $R_\ell[X]$-module and $\ker(\psi)$ is only an R_ℓ-module. Hence multiplication by X needs to be dealt with when transferring a generating set of N to a generating set of $\ker(\psi)$. For this purpose, set $R_\ell[X]^{<d} = \{\, f \in R_\ell[X] \mid \deg(f) < d \,\}$. Then

$$\begin{aligned} \varphi : R_\ell[X]^{<d} &\overset{\sim}{\longrightarrow} R_\ell^d \\ X^{i-1} &\longmapsto \mathbf{e}_i \end{aligned} \tag{3.4}$$

is an R_ℓ-module isomorphism. Let

$$\mathsf{N}^{<d} = \{\, f \in \mathsf{N} \mid \deg(f) < d \,\}$$

be the set of all elements in N of degree less than d. Then $\mathsf{N}^{<d}$ is an R_ℓ-module, and for $f_1, \dots, f_r \in R_\ell[X]^{<d}$, the following holds

$$\mathsf{N}^{<d} = \langle f_1, \dots, f_r \rangle_{R_\ell} \quad\Longleftrightarrow\quad \ker(\psi) = \langle \varphi(f_1), \dots, \varphi(f_r) \rangle_{R_\ell}$$

according to the equivalence in (3.3). We modify the sequence in (3.2) accordingly to get the following exact sequence of R_ℓ-modules.

$$\begin{aligned} \mathbf{0} \longrightarrow \mathsf{N}^{<d} \longrightarrow R_\ell[X]^{<d} &\longrightarrow R_\ell[A] \longrightarrow \mathbf{0} \\ X^i &\longmapsto A^i \end{aligned} \tag{3.5}$$

The following lemma describes which $R_\ell[X]$-generating sets of N can be transferred to R_ℓ-generating sets of $\mathsf{N}^{<d}$.

Lemma 3.4. *Let $A \in \mathrm{M}_n(R_\ell)$ be a square matrix over R_ℓ and d the degree of a (p^ℓ)-minimal polynomial of A. Further, let $f_1, \dots, f_m$ be a generating set of the null ideal N of A in $R_\ell[X]$ such that*

1. $\deg(f_1) < \cdots < \deg(f_m) = d$,
2. *$f_i = [p^{t_i}]_{p^\ell}\, g_i$ for monic polynomials $g_i \in R_\ell[X]$ $(1 \le i \le m)$ and natural numbers $t_1 > \cdots > t_m$,*

3. $f \in \sum_{i \in \mathcal{I}^{[f]}} f_i\, R_\ell[X]$ *for all* $f \in \mathsf{N}$*, where* $\mathcal{I}^{[f]} = \{\, 1 \le i \le m \mid \deg(f_i) \le \deg(f) \,\}$.

Then

$$\mathsf{N}^{<d} = \sum_{i=1}^{m-1} \sum_{t=1}^{s_i} (X^{t-1} f_i)\, R_\ell$$

where $s_i = \deg(f_{i+1}) - \deg(f_i)$*.*

Proof. The conditions on the degrees of the polynomials f_i guarantee that $\deg(X^{t-1} f_i) < d$ for $1 \le i \le m-1$ and $1 \le t \le s_i$. Hence the inclusion "$\supseteq$" is easily seen and it suffices to show "$\subseteq$". Let $f \in \mathsf{N}^{<d}$. We prove this by induction on $\deg(f)$.
For the basis, let $0 \neq f \in \mathsf{N}^{<d}$ be a polynomial of minimal degree in $\mathsf{N}^{<d}$, that is, $\deg(f) \le \deg(g)$ for all $g \in \mathsf{N}^{<d}$. Since

$$f \in \sum_{i \in \mathcal{I}^{[f]}} f_i\, R_\ell[X]$$

it follows that $\mathcal{I}^{[f]} = \{\, 1 \le i \le m \mid \deg(f_i) \le \deg(f) \,\} \neq \emptyset$. Therefore $\deg(f) = \deg(f_1)$ and $\mathcal{I}^{[f]} = \{1\}$ (since $\deg(f_j) > \deg(f_1)$ for $j > 1$). Hence $f = r f_1$ for $r \in R_\ell$ which proves the basis.
Assume now $f \in \mathsf{N}^{<d}$ with $\deg(f) > \deg(f_1)$. Let $1 \le k < m$ such that $\deg(f_k) \le \deg(f) < \deg(f_{k+1})$. Then, $f \in \sum_{i=1}^{k} f_i R_\ell[X] \subseteq p^{t_k} R_\ell[X]$ according to our assumptions on the polynomials f_i (where we write p for its residue class $[p]_{p^\ell}$). Let $f' \in R_\ell[X]$ (with $\deg(f) = \deg(f')$) such that $f = p^{t_k} f'$. Since $f_k = p^{t_k} g_k$ for a monic polynomial $g_k \in R_\ell[X]$, there exist $q, r \in R_\ell[X]$ with $\deg(r) < \deg(g_k) = \deg(f_k)$ such that

$$f' = q g_k + r. \tag{3.6}$$

Therefore

$$f = q f_k + p^{t_k} r$$

which implies $p^{t_k} r \in \mathsf{N}^{<d}$, and we can apply the induction hypothesis to $p^{t_k} r$. Hence

$$p^{t_k} r \in \sum_{i=1}^{m-1} \sum_{t=1}^{s_i} (X^{t-1} f_i)\, R_\ell.$$

Since $\deg(f') = \deg(f) < \deg(f_{k+1})$, Equation (3.6) implies $\deg(q) = \deg(f) - \deg(f_k) < \deg(f_{k+1}) - \deg(f_k) = s_k$. Therefore

$$q f_k \in \sum_{t=1}^{s_k} (X^{t-1} f_k) R_\ell$$

and the assertion follows for $f = q f_k + p^{t_k} r$. □

According to Corollary 2.21, any generating set of the form $\{\, p^{\ell-i}\nu_i \mid i \in \mathcal{I}_\ell^\star \,\}$, where $\nu_i \in R_\ell[X]$ are (p^i)-minimal polynomials, satisfies the conditions of Lemma 3.4. This allows us to prove the following theorem which is the main result of this section.

Theorem 3.5. *Let $A \in \mathrm{M}_n(R_\ell)$ and $\nu_i \in R_\ell[X]$ be (p^i)-minimal polynomials with $d_i = \deg(\nu_i)$ for $0 \le i \le \ell$. Then*

$$R_\ell[A] \simeq \bigoplus_{i=0}^{\ell-1} (R_{\ell-i})^{d_{i+1}-d_i}.$$

Further, let $\mathcal{I}_\ell^\star$ be the reduced index set of A and $s_i = \deg(\nu_{\mathrm{succ}(i)}) - \deg(\nu_i)$ for $i \in \mathcal{I}_\ell^\star$, then

$$R_\ell[A] \simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{i \in \mathcal{I}_\ell^\star} (R_{\ell-i})^{s_i}$$

where $\mathsf{d}_p = \deg(\nu_1)$ is the p-degree of A.

Proof. First, we show that the two decompositions of $R_\ell[A]$ given in the theorem, are isomorphic. Recall that $\nu_0 = 1$ and $d_0 = 0$. Hence $R_\ell^{\mathsf{d}_p} = R_{\ell-i}^{d_{i+1}-d_i}$ for $i = 0$. Let now $i \ge 1$. By Remark 3.3, an element $1 \le i < \ell$ is in the reduced index set $\mathcal{I}_\ell^\star$ of A if and only if $d_i < d_{i+1}$, and if one of these equivalent conditions is satisfied, then $d_{i+1} = d_{\mathrm{succ}(i)}$. Therefore, $i \in \mathcal{I}_\ell^\star$ if and only if $R_{\ell-i}^{d_{i+1}-d_i} \neq \mathbf{0}$ and then $(R_{\ell-i})^{s_i} = (R_{\ell-i})^{d_{i+1}-d_i}$. Hence the two representations are isomorphic and it suffices to show that

$$R_\ell[A] \simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{i \in \mathcal{I}_\ell^\star} (R_{\ell-i})^{s_i}.$$

According to Corollary 2.21 the polynomials in $\{\, p^{\ell-i}\nu_i \mid i \in \mathcal{I}_\ell^\star \,\}$ satisfy the conditions of Lemma 3.4, and therefore

$$\mathsf{N}^{<d} = \sum_{i \in \mathcal{I}_\ell^\star} \sum_{t=1}^{s_i} (p^{\ell-i} X^{t-1} \nu_i)\, R_\ell.$$

Since $s_i = \deg(\nu_{\mathrm{succ}(i)}) - \deg(\nu_i)$, it follows that

$$\begin{array}{rcl} \delta : \{\, (i,t) \mid i \in \mathcal{I}_\ell^\star, 1 \le t \le s_i \,\} & \xrightarrow{\sim} & \{\, \mathsf{d}_p + 1, \ldots, d \,\} \\ (i,t) & \longmapsto & \deg(\nu_i) + t \end{array}$$

is a bijection. For $1 \le j \le d$, we define

$$\mathbf{b}_j = \begin{cases} X^{j-1} & \text{if } 1 \le j \le \mathsf{d}_p \\ X^{t-1}\nu_i & \text{if } \mathsf{d}_p + 1 \le j = \delta(i,t) \le d\ . \end{cases}$$

Observe that $\deg(\mathbf{b}_j) = j-1$. Hence $\mathbf{b}_1, \dots, \mathbf{b}_d$ is a basis of $R_\ell[X]^{<d}$. Together with the exact sequence (3.5), this implies

$$\begin{aligned} R_\ell[A] &\simeq {}^{R_\ell[X]^{<d}}\!/\mathsf{N}^{<d} \\ &\simeq \bigoplus_{i=1}^{\mathsf{d}_p} \mathbf{b}_i\, R_\ell \oplus \bigoplus_{i\in\mathcal{I}_\ell^\star} \bigoplus_{t=1}^{s_i} {}^{\mathbf{b}_{\delta(i,t)} R_\ell}\!/\!_{(p^{\ell-i}\,\mathbf{b}_{\delta(i,t)})R_\ell} \\ &\simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{i\in\mathcal{I}_\ell^\star} (R_{\ell-i})^{s_i} \ . \end{aligned}$$

□

Remark 3.6. Let the notation be as in Theorem 3.5. If $\mathcal{I}_\ell^\star = \{i_1, \dots, i_r\}$ with $i_1 < \cdots < i_r < i_{r+1} = \ell$. Then $s_{i_j} = \deg(\nu_{i_{j+1}}) - \deg(\nu_{i_j})$ for $1 \le j \le r$. According to Theorem 3.5, the uniquely determined invariant factors of $R_\ell[A]$ (with multiplicities) are

$$\underbrace{1,\dots,1}_{\mathsf{d}_p},\underbrace{p^{\ell-i_1},\dots,p^{\ell-i_1}}_{s_{i_1}},\dots,\underbrace{p^{\ell-i_r},\dots,p^{\ell-i_r}}_{s_{i_r}}.$$

Note that the occurring exponents $\ell - i_1, \dots, \ell - i_r$ of the invariant factors correspond to the elements of the set $\mathcal{I}_\ell^\star$. Further, if $\nu_k \in R_\ell[X]$ is a (p^k)-minimal polynomial of A (for $1 \le k \le \ell$), then there exists $1 \le u \le r+1$ such that $\deg(\nu_k) = \deg(\nu_{i_u})$ and

$$\deg(\nu_k) = \sum_{i=0}^{k-1} (d_{i+1} - d_i) = \mathsf{d}_p + \sum_{j=1}^{u-1} s_{i_j}.$$

Recall that the ℓ-th index set of a matrix defines a generating set of the null ideal $\mathsf{N}^{R_\ell}(A)$ of A consisting of polynomials of the form $p^{\ell-j}\nu_j$. Per definition, $\mathcal{I}_\ell^\star$ depends on the degrees of these polynomials. In particular, observe that $\mathcal{I}_\ell^\star = \emptyset$ if and only if $\deg(\nu_\ell) = \deg(\nu_1) = \mathsf{d}_p$. Together with Theorems 2.19 and 3.5 this implies the following corollary.

Corollary 3.7. *Let $A \in \mathrm{M}_n(R_\ell)$ with ℓ-th index set $\mathcal{I}_\ell$, (p^ℓ)-minimal polynomial ν_ℓ and p-degree d_p. Then the following assertions are equivalent:*

1. $R_\ell[A] \simeq R_\ell^{\mathsf{d}_p}$
2. $\deg(\nu_\ell) = \mathsf{d}_p$
3. $\mathsf{N}^{R_\ell}(A) = \nu_\ell R_\ell[X]$

We can reformulate this in terms of matrices with entries in D.

Corollary 3.8. *Let $A \in \mathrm{M}_n(D)$ and $\ell \in \mathbb{N}$. Further, let $\nu_j \in D[X]$ be (p^j)-minimal polynomials of A for $1 \le j \le \ell$ and $[A]_{p^j}$ be the image of A under projection modulo p^j. The following assertions are equivalent.*

1. $\mathsf{N}_{p^\ell}^D(A) = \nu_\ell D[X] + p^\ell D[X]$.

2. $\mathsf{N}_{p^j}^D(A) = \nu_j D[X] + p^j D[X]$ *for all* $1 \leq j \leq \ell$.

3. $R_j[[A]_{p^j}] \simeq R_j^{\mathsf{d}_p}$ *for all* $1 \leq j \leq \ell$.

4. $\deg(\nu_\ell) = \mathsf{d}_p$.

5. ν_ℓ *is a* (p^j)*-minimal polynomial of* A *for all* $1 \leq j \leq \ell$.

Recall, that Proposition 2.22 states, that for $A \in \mathrm{M}_n(D)$, there exists $m \in \mathbb{N}$ such that $\deg(\nu_{m+k}) = \deg(\nu_A)$ for all $k \geq 0$. Then $\mathcal{I}_{m+k}^\star = \mathcal{I}_m^\star$, cf. Remark 2.18. Together with Theorem 3.5 we conclude this section with a final corollary.

Corollary 3.9. *Let* $A \in \mathrm{M}_n(D)$ *and* ν_j *be* (p^j)*-minimal polynomials for* $j \geq 1$*. Further, let* $[A]_{p^j}$ *be the image of* A *under projection modulo* p^j*. Then there exists* $m \in \mathbb{N}$ *such that for all* $\ell \geq m$ *the following holds*

$$R_\ell[[A]_{p^\ell}] \simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{j \in \mathcal{I}_m^\star} (R_{\ell-j})^{s_j}$$

where $\mathcal{I}_m^\star$ *is the reduced index set of* $[A]_{p^m}$ *and* $s_j = \deg(\nu_{\mathrm{succ}(j)}) - \deg(\nu_j)$ *for* $j \in \mathcal{I}_m^\star$*. In particular,* $R_\ell[[A]_{p^\ell}]$ *decomposes into* $\deg(\mu_A)$ *non-zero cyclic summands.*

4 Integer-valued polynomials on one matrix

This section is dedicated to the application of the results of Section 2 in the context of integer-valued polynomials on a single matrix. Again, let D be a principal ideal domain with quotient field K and $A \in \mathrm{M}_n(D)$ be a square matrix with entries in D. We want to determine the ring $\mathrm{Int}(A, \mathrm{M}_n(D))$ of all integer-valued polynomials on A, that is,

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \{\, f \in K[X] \mid f(A) \in \mathrm{M}_n(D) \,\}.$$

Once we have an explicit description of $\mathrm{Int}(A, \mathrm{M}_n(D))$, we can determine the ring of images of A under $\mathrm{Int}(A, \mathrm{M}_n(D))$, that is,

$$\text{Int-Im}(A, \mathrm{M}_n(D)) = \{\, f(A) \mid f \in \mathrm{Int}(A, \mathrm{M}_n(D)) \,\}.$$

For the ring of integer-valued polynomials on a single matrix A, the following inclusion holds

$$\mu_A K[X] + D[X] \subseteq \mathrm{Int}(A, \mathrm{M}_n(D)).$$

There are both instances in which equality holds, and instances in which the inclusion is strict. If equality holds, it is readily seen that $\text{Int-Im}(A, \mathrm{M}_n(D)) = D[A]$, that is, all images of A under integer-valued polynomials on A can be written as $g(A)$ with $g \in D[X]$. As far as the images of A are concerned, the integer-valued polynomials in $K[X] \setminus D[X]$ do not contribute anything new in this case. In fact, as the next proposition states, the reverse implication holds too. (Thanks to Giulio Peruginelli for pointing this out.)

Proposition 4.1. *Let D be a principal ideal domain and $A \in \mathrm{M}_n(D)$ with minimal polynomial $\mu_A \in D[X]$. Then the following assertions are equivalent:*

1. $\mathrm{Int}(A, \mathrm{M}_n(D)) = \mu_A K[X] + D[X]$

2. $\forall\, f \in \mathrm{Int}(A, \mathrm{M}_n(D)) \setminus D[X] :\ \deg(f) \geq \deg(\mu_A)$

3. $\text{Int-Im}(A, \mathrm{M}_n(D)) = D[A]$

Proof. For the implication from *1.* to *2.* let $f \in \mathrm{Int}(A, \mathrm{M}_n(D)) \setminus D[X]$, then there exist $h \in K[X]$ and $g \in D[X]$ such that $f = h\mu_A + g$. Since $\mu_A \in D[X]$, we can assume that $\deg(g) < \deg(\mu_A)$. Further, $f \notin D[X]$ implies that $f \neq g$ and $h \neq 0$. Therefore $\deg(f) = \deg(h) + \deg(\mu_A) \geq \deg(\mu_A)$.
For the implication *2.* to *3.* let $f \in \mathrm{Int}(A, \mathrm{M}_n(D))$. By polynomial division, there exists $q, r \in K[X]$ such that $f = q\mu_A + r$ and $\deg(r) < \deg(\mu_A)$. The assumption in *2.* implies that $r \in D[X]$ and therefore $f(A) = r(A) \in D[A]$.
And finally we show that *3.* implies *1.* Again, let $f \in \mathrm{Int}(A, \mathrm{M}_n(D))$. Then, since $\text{Int-Im}(A, \mathrm{M}_n(D)) = D[A]$ holds by assumption, there exists $g \in D[X]$ such that $f(A) = g(A)$. This further implies that $f - g \in \mathsf{N}^K(A) = \mu_A K[X]$ and hence there exists $h \in K[X]$ such that $f - g = h\mu_A$. The assertion follows. □

Remark 4.2. The result above holds more generally over arbitrary domains D under the additional assumptions that the minimal polynomial μ_A is an element of $D[X]$. Moreover, it is worth mentioning this assumption is only needed in the proof of the implication from *1.* to *2.*

However, in general, $\deg(\mu_A)$ is not a lower bound for the degree of polynomials in $\mathrm{Int}(A, \mathrm{M}_n(D)) \setminus D[X]$. Let $f = \frac{g}{d} \in K[X]$ with $g \in D[X]$ and $d \in D$ and $d = \prod_{i=1}^{m} p_i^{\ell_i}$ the prime factorization of d. Then the following assertions are equivalent:

1. $f \in \mathrm{Int}(A, \mathrm{M}_n(D))$
2. $g(A) \equiv 0 \mod d\,\mathrm{M}_n(D)$
3. $g(A) \equiv 0 \mod p_i^{\ell_i}\, \mathrm{M}_n(D)$ for all $1 \leq i \leq m$

The results of Section 2 provide the tools to give an explicit description of the ring $\mathrm{Int}(A, \mathrm{M}_n(D))$ of integer-valued polynomials on A.

Theorem 4.3. *Let D be a principal ideal domain and $A \in \mathrm{M}_n(D)$ with minimal polynomial $\mu_A \in D[X]$. Then there exists a finite set $\mathcal{P}_A \subset \mathbb{P}$ of prime elements of D and natural numbers $m_p \in \mathbb{N}$ for $p \in \mathcal{P}_A$ such that*

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \mu_A K[X] + D[X] + \sum_{p \in \mathcal{P}_A} \sum_{j \in \mathcal{I}_{(p,m_p)}} \frac{\nu_{(p,j)}}{p^j} D[X]$$

where $\nu_{(p,j)} \in D[X]$ are (p^j)-minimal polynomials of A for $j \geq 0$, and $\mathcal{I}_{(p,m_p)}$ is the m_p-th index set of A with respect to the prime p.

Proof. It suffices to show "$\subseteq$". Recall that $\mathsf{N}_d(A) = \mathsf{N}_d^D(A) = \{\, f \in D[X] \mid f(A) \in d\,\mathrm{M}_n(D) \,\}$ and that $\mathsf{N}_0(A) = \mathsf{N}(A) = \mu_A D[X] \subseteq D[X] = \mathsf{N}_1(A)$ and hence

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \sum_{d \in D \setminus \{0\}} \frac{1}{d}\, \mathsf{N}_d(A).$$

According to Lemma 2.9, this implies

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \sum_{p \in \mathbb{P}} \sum_{\ell \in \mathbb{N}} \frac{1}{p^\ell}\, \mathsf{N}_{p^\ell}(A). \tag{4.1}$$

First, we show that there exists a finite subset $\mathcal{P}_A \subseteq \mathbb{P}$ such that the following holds

$$\forall\, p \in \mathbb{P} \setminus \mathcal{P}_A :\ \mathsf{N}_{p^\ell}(A) = \mu_A D[X] + p^\ell D[X]. \tag{4.2}$$

Considered as a matrix over K, A is similar to its rational canonical form C, cf. [16]. Let $\mu_1 \mid \cdots \mid \mu_r = \mu_A$ be the invariant factors of A. Then there exists a matrix $T \in \mathrm{GL}_n(K)$ such that

$$T^{-1}AT = C = \mathcal{C}_{\mu_A} \oplus \cdots \oplus \mathcal{C}_{\mu_1}$$

where $\mathcal{C}_f$ denotes the companion matrix of a monic polynomial f. Since D is a principal ideal domain, it is integrally closed. As mentioned above, this implies $\mu_A \in D[X]$. Indeed, this implies that $\mu_i \in D[X]$ for all $1 \le i \le r$, since they are all monic divisors of the characteristic polynomial $\chi_A \in D[X]$, cf. [3, Ch. 5, §1.3, Prop. 11]. Therefore the rational canonical form C of A is a matrix with entries in D.

However, in general, A is not similar to C over the domain D, that is, we cannot assume $T \in \mathrm{GL}_n(D)$. Let $\mathcal{P}_A \subseteq \mathbb{P}$ be the set of prime elements which occur as divisors of the denominators of the entries of T or its inverse T^{-1}. Then $\mathcal{P}_A$ is finite and T, T^{-1} are invertible matrices over the localization $D_{(p)}$ of D at p for all $p \in \mathbb{P} \setminus \mathcal{P}_A$ and we can reduce the equation above modulo all $p \in \mathbb{P} \setminus \mathcal{P}_A$:

$$[T]_p^{-1}[A]_p[T]_p = [T^{-1}AT]_p = [C]_p = \mathcal{C}_{[\mu_A]_p} \oplus \cdots \oplus \mathcal{C}_{[\mu_1]_p}$$

(where we identify the residue fields of D and $D_{(p)}$ modulo p). It is well known, that a monic polynomial f is the minimal polynomial of its companion matrix $\mathcal{C}_f$ over any domain. Therefore $[\mu_A]_p$ is the minimal polynomial of $\mathcal{C}_{[\mu_A]_p}$. Further, $[\mu_A]_p(\mathcal{C}_{[\mu_i]_p}) = 0$ holds since $\mu_i \mid \mu_A$ for all $1 \le i \le m$. Hence μ_A is a (p)-minimal polynomial for all $p \in \mathbb{P} \setminus \mathcal{P}_A$, which implies the assertion in (4.2) above, according to Corollary 3.8.

Thus, Equations (4.1) and (4.2) imply

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \mu_A K[X] + D[X] + \sum_{p \in \mathcal{P}_A} \sum_{\ell \ge 1} \frac{1}{p^\ell}\, \mathsf{N}_{p^\ell}(A). \tag{4.3}$$

Further, by Corollary 2.23, for all prime elements $p \in \mathcal{P}_A$, there exists $m_p \in \mathbb{N}$ such that for all $\ell \ge m_p$

$$\mathsf{N}_{p^\ell}(A) = \mu_A D[X] + p^{\ell - m_p}\mathsf{N}_{p^{m_p}}(A)$$

holds, and we can restrict the inner sum in Equation (4.3) to all $1 \leq \ell \leq m_p$. And finally, since $p\mathsf{N}_{p^{\ell-1}}(A) \subseteq \mathsf{N}_{p^\ell}(A)$, it follows hat $\frac{1}{p^{\ell-1}}\mathsf{N}_{p^{\ell-1}}(A) \subseteq \frac{1}{p^\ell}\mathsf{N}_{p^\ell}(A)$. Hence

$$\sum_{\ell=1}^{m_p} \frac{1}{p^\ell}\mathsf{N}_{p^\ell}(A) = \frac{1}{p^{m_p}}\mathsf{N}_{p^{m_p}}(A).$$

Then, Theorem 2.19 implies

$$\operatorname{Int}(A, \mathrm{M}_n(D)) = \mu_A K[X] + D[X] + \sum_{p \in \mathcal{P}_A} \sum_{j \in \mathcal{I}_{(p,m_p)}} \frac{\nu_{(p,j)}}{p^j} D[X].$$

□

Corollary 4.4. *Let D be a principal ideal domain and $A \in \mathrm{M}_n(D)$ with minimal polynomial $\mu_A \in D[X]$. Then there exists a finite set $\mathcal{P}_A \subset \mathbb{P}$ and natural numbers $m_p \in \mathbb{N}$ for $p \in \mathcal{P}_A$ such that*

$$\text{Int-Im}(A, \mathrm{M}_n(D)) = D[A] + \sum_{p \in \mathcal{P}_A} \sum_{j \in \mathcal{I}_{(p,m_p)}} \frac{\nu_{(p,j)}(A)}{p^j} D[A]$$

where $\nu_{(p,j)} \in D[X]$ are (p^j)-minimal polynomial of A for $j \geq 0$, and $\mathcal{I}_{(p,m_p)}$ is the m_p-th index set of A with respect to the prime p.

Example 4.5. We continue Example 2.27, and determine the rings $\operatorname{Int}(A, \mathrm{M}_3(\mathbb{Z}))$ of integer-valued polynomials on A and $\text{Int-Im}(A, \mathrm{M}_3(\mathbb{Z}))$ of integer-valued images for

$$A = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 16 & 0 \\ 0 & 0 & 32 \end{pmatrix} \in \mathrm{M}_3(\mathbb{Z}).$$

We know that

$$\operatorname{Int}(A, \mathrm{M}_3(\mathbb{Z})) = \sum_{p \in \mathbb{P}} \sum_{\ell \in \mathbb{N}} \frac{1}{p^\ell} \mathsf{N}_{p^\ell}(A).$$

We can use the data of Example 2.27 in order to conclude that

$$\begin{aligned} \operatorname{Int}(A, \mathrm{M}_3(\mathbb{Z})) &= \mu_A \mathbb{Q}[X] + \mathbb{Z}[X] + \frac{1}{3}\mathsf{N}_3(A) + \frac{1}{7}\mathsf{N}_7(A) + \frac{1}{64}\mathsf{N}_{64}(A) \\ &= \mu_A \mathbb{Q}[X] + \mathbb{Z}[X] + \sum_{p \in \{2,3,7\}} \frac{1}{p^{m_p}} \mathsf{N}_{p^{m_p}}(A) \end{aligned}$$

where $m_2 = 6$ and $m_3 = m_7 = 1$. Similarly to the computation in Example 2.27 it follows that the $\{0, 1, \ell\}$ is the ℓ-th index set of A with respect to 7 (for $\ell \geq 1$) and

$(X-4)(X-16)$ is a (7)-minimal polynomial of A (since $4, 16, 32, \dots$ is a 7-ordering of $\{4, 16, 32\}$, cf. Example 2.27). Hence

$$\begin{aligned}\mathrm{Int}(A, \mathrm{M}_3(\mathbb{Z})) =& (X-4)(X-16)(X-32)\mathbb{Q}[X] + \mathbb{Z}[X] \\ &+ \frac{1}{3}(X-4)(X-32)\mathbb{Z}[X] + \frac{1}{7}(X-4)(X-16)\mathbb{Z}[X] \\ &+ \frac{1}{64}(X-4)(X-16)\mathbb{Z}[X] + \frac{1}{4}(X-4)\mathbb{Z}[X].\end{aligned}$$

And finally, this implies

$$\begin{aligned}\mathrm{Int}(A, \mathrm{M}_3(\mathbb{Z}))(A) = \mathbb{Z}[A] &+ \begin{pmatrix} 0 & 0 & 0 \\ 0 & -64 & 0 \\ 0 & 0 & 0 \end{pmatrix}\mathbb{Z}[A] + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 64 \end{pmatrix}\mathbb{Z}[A] \\ &+ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 7 \end{pmatrix}\mathbb{Z}[A] + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{pmatrix}\mathbb{Z}[A].\end{aligned}$$

References

[1] M. Bhargava. P-orderings and polynomial functions on arbitrary subsets of Dedekind rings. *J. Reine Angew. Math.*, 490:101–127, 1997.

[2] M. Bhargava. The factorial function and generalizations. *Amer. Math. Monthly*, 107(9):783–799, 2000.

[3] N. Bourbaki. *Commutative Algebra, Chapters 1-7.* Springer, Berlin, 1989.

[4] W. C. Brown. *Matrices over Commutative Rings.* Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, Inc., New York, 1993.

[5] W. C. Brown. Null ideals and spanning ranks of matrices. *Comm. Algebra*, 26(8):2401–2417, 1998.

[6] W. C. Brown. Null ideals and spanning ranks of matrices. II. *Comm. Algebra*, 27(12):6051–6067, 1999.

[7] W. C. Brown. Null ideal of matrices. *Comm. Algebra*, 33:4491 – 4504, 2005.

[8] S. Evrard, Y. Fares, and K. Johnson. Integer valued polynomials on lower triangular integer matrices. *Monatsh. Math.*, 170:147–160, 2013.

[9] S. Frisch. Integrally closed domains, minimal polynomials, and null ideals of matrices. *Communications in Algebra*, 32(5):2015–2017, 2004.

[10] S. Frisch. Integer-valued polynomials on algebras - a survey. *Actes du CIRM*, 2:27–32, 2010.

[11] S. Frisch. Integer-valued polynomials on algebras. *J. Algebra*, 373:414–425, 2013.

[12] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2002.

[13] K. A. Loper and N. J. Werner. Generalized rings of integer-valued polynomials. *J. Number Theory*, 132(11):2481–2490, 2012.

[14] G. Peruginelli. Integer-valued polynomials over matrices and divided differences. *Monatsh. Math.*, 173(4):559–571, 2014.

[15] G. Peruginelli and N. Werner. Integral closure of rings of integer-valued polynomials on algebras. In *Commutative Algebra: Recent Advances in Commutative Rings, Integer-Valued Polynomials, and Polynomial Functions*. Springer, 2014. Editors: Fontana, M. and Frisch, S. and Glaz, S.

[16] S. Roman. *Advanced Linear Algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 3rd edition, 2008.